WHAT IS CLAIMED IS:

1. A method for privately communicating over a wireless communications network, comprising the steps of:

processing the communication signals in a first signal processing circuit within a first communications controller circuit at a first location to produce processed communication signals;

enciphering the processed communication signals in the first signal processing circuit to produce enciphered and processed communication signals;

transmitting the enciphered and processed communication signals between a first location and a second location using the first communications controller circuit;

receiving the enciphered and processed communication signals at the second location using a second communications controller circuit;

deciphering the enciphered and processed communication signals in a second signal processing circuit within the second communications controller circuit; and

processing the deciphered and processed communication signals in the second signal processing circuit to produce communications signals at the second location.

2. The method of Claim 1, wherein said enciphering step further comprises the steps of:

embedding an enciphering algorithm within the first signal processing circuit; and

enciphering the processed communication signals using the embedded enciphering algorithm.

3. The method of Claim 2, wherein said deciphering step further comprises the steps of:

embedding a deciphering algorithm within the second signal processing circuit; and

deciphering said processed communication signals using said embedded deciphering algorithm.

4. The method of Claim 2, wherein said enciphering step comprises the step of embedding the enciphering algorithm in said first signal processing circuit after manufacturing said first communications controller circuit.

5. The method of Claim 2, wherein said enciphering step further comprises the step of enciphering the process communication signals in a dedicated signal processing unit of the first signal processing circuit, dedicated signal processing unit being tasked to perform said enciphering step.

6. The method of Claim 2, wherein said enciphering algorithm embedding step comprises the step of embedding an F enciphering algorithm in said first signal processing circuit.

7. The method of Claim 2, wherein said enciphering algorithm embedding step comprises the step of embedding a DES enciphering algorithm in said first signal processing circuit.

8. The method of Claim 2, wherein said enciphering algorithm embedding step comprises the step of embedding a BONUS enciphering algorithm in said first signal processing circuit.

9. The method of Claim 2, wherein said enciphering algorithm embedding step comprises the step of embedding a DECT standard enciphering algorithm in said first signal processing circuit.

10. The method of Claim 1, wherein said enciphering step further comprises the step of enciphering said processed communication signals in said first signal processing circuit by programmably selecting an enciphering algorithm.

11. The method of Claim 10, wherein said programmably selecting step further comprises the step of programmably selecting the enciphering algorithm from among the group consisting essentially of an F enciphering algorithm, a DES enciphering algorithm, and a BONUS enciphering algorithm.

12. The method of Claim 10, wherein said deciphering step further comprises the step of deciphering the processed communication signals in a dedicated signal processing unit of the first signal processing circuit, the dedicated signal processing unit being tasked to perform said deciphering step.

13. The method of Claim 1, wherein said deciphering step comprises the step of embedding said deciphering algorithm in said second signal processing circuit after manufacturing said first communications controller circuit.

14. The method of Claim 13, wherein said deciphering algorithm embedding step comprises the step of embedding an F deciphering algorithm in said second signal processing circuit for deciphering communication signals first enciphered using an F enciphering algorithm.

15. The method of Claim 13, wherein said deciphering algorithm embedding step comprises the step

of embedding a DES deciphering algorithm in said second signal processing circuit for deciphering communication signals first enciphered using a DES enciphering algorithm.

16. The method of Claim 13, wherein said enciphering algorithm embedding step comprises the step of embedding a DECT standard enciphering algorithm in said first signal processing circuit.

17. The method of Claim 13, wherein said deciphering algorithm embedding step comprises the step of embedding a BONUS deciphering algorithm in said second signal processing circuit for deciphering communication signals first enciphered using a BONUS enciphering algorithm.

18. The method of Claim 1, further comprising the step of generating authentication signals from said first location, comprising performing in said first signal processing circuit the steps of:

generating a first location identifier;

receiving a randomly generated number from said second location;

employing a privacy function on said randomly generated number and said first location identifier to generate an enciphered value; and

directing said enciphered value to said second communications controller circuit.

19. The method of Claim 1, further comprising the step of authenticating said communication signals from said first location, said authenticating step comprising performing in said second signal processing circuit the steps of:

generating said first location identifier;

randomly generating said randomly generated number;

employing a privacy function on said randomly generated number and said first location identifier to generate an expected enciphered value;

receiving said enciphered value from said first location;

comparing said expected enciphered value to said enciphered value; and

generating an authentication signal in the event that said expected enciphered value matches said enciphered value.

20. The method of Claim 1, further comprising the step of XOR-ing said enciphered and processed communication signals with clear processed communication signals for preventing propagation of single-bit errors from said first signal processing circuit to said second signal processing circuit.

21. A system for privately communicating communications signals over a wireless communications network, comprising:

a first communications controller at a first location;

a first signal processing circuit within a first communications controller circuit for processing communications signals to form processed communication signals and further enciphering said processed communication signals;

a first transceiver associated with said first communications controller for transmitting said enciphered and processed communication signals between said first location;

a second communications controller circuit for controlling communications at said second location;

a second transceiver associated with said second communications circuit for receiving said enciphered and processed communication signals from said first transceiver;

a second signal processing circuit within said second communications controller circuit for deciphering said received enciphered and processed communication signals, said second signal processing circuit further for processing said deciphered and processed communication signals.

22. The system of Claim 21, wherein said first signal processing circuit comprises a first digital signal processing circuit.

23. The system of Claim 22, further comprising a dedicated digital signal processor within said first digital signal processing circuit for enciphering said processed communication signals.

24. The system of Claim 21, wherein said second signal processing circuit comprises a second digital signal processing circuit.

25. The system of Claim 24, further comprising a dedicated digital signal processor within said second digital signal processing circuit for deciphering said enciphered and processed communication signals.

26. The system of Claim ~~19~~ 21, further comprising an enciphering algorithm embedded within said first signal processing circuit for enciphering said processed communication signals.

27. The system of Claim 22, wherein said first signal processing circuit further comprises circuitry and instructions for embedding said enciphering algorithm in said first signal processing circuit after first manufacturing said first communications controller circuit.

28. The system of Claim 23, wherein said first signal processing circuit comprises circuitry and instructions for embedding an F enciphering algorithm in said first signal processing circuit.

29. The system of Claim 23, wherein said first signal processing circuit comprises circuitry and instructions for embedding a DES enciphering algorithm in said first signal processing circuit.

30. The system of Claim 23, wherein said first signal processing circuit comprises circuitry and instructions for embedding a BONUS enciphering algorithm in said first signal processing circuit.

31. The method of Claim 23, wherein said enciphering algorithm embedding step comprises the step of embedding a DECT standard enciphering algorithm in said first signal processing circuit.

32. The system of Claim 23, further comprising a deciphering algorithm within said second signal processing circuit for deciphering said enciphered and processed communication signals.

33. The system of Claim 23, wherein said first signal processing circuit comprises circuitry and instructions for enciphering said processed communication signals in said first signal processing circuit by programmably selecting an enciphering algorithm.

34. The system of Claim 29, said first signal processing circuit further comprises circuitry and instructions for programmably selecting the enciphering algorithm from among the group consisting essentially of an F enciphering algorithm, a DES enciphering algorithm, and a BONUS enciphering algorithm.

35. The system of Claim 21, wherein said second communications controller circuit further comprises circuitry and instructions for embedding said deciphering algorithm within said second signal processing circuit after first manufacturing said second communications controller circuit.

36. The system of Claim 31, wherein said deciphering algorithm comprises an F deciphering algorithm embedded within said second signal processing circuit for deciphering communications signals first enciphered using an F enciphering algorithm.

37. The system of Claim 31, wherein said deciphering algorithm comprises a DES deciphering algorithm embedded within said second signal processing circuit for deciphering communications signals first enciphered using an DES enciphering algorithm.

38. The system of Claim 31, wherein said deciphering algorithm comprises a BONUS deciphering algorithm embedded within said second signal processing circuit for deciphering communications signals first enciphered using an BONUS enciphering algorithm.

39. The method of Claim 31, wherein said enciphering algorithm embedding step comprises the step of embedding a DECT standard enciphering algorithm in said first signal processing circuit.

40. The system of Claim 23, further comprising circuitry and instructions within said first signal processing circuit for authenticating communications between said first location and said second location:

instructions within said first communications controller circuit for generating a first location identifier;

receiving circuitry associated with said first communications controller for receiving a randomly generated number from said second location;

privacy instructions embedded within said first signal processing circuit for employing a privacy function on said randomly generated number and said first location identifier at said to generate an enciphered value; and

communications circuitry for directing said enciphered value to said second communications controller circuit.

41. The system of Claim 21, further comprising within said second communications controller circuit instructions for authenticating said generated authentication signals from said first location said authenticating instructions, comprising:

identifier generating instructions for generating said first location identifier;

random number generating instructions for randomly generating said randomly generated number;

privacy function instructions for transforming said randomly generated number and said first location identifier into an expected enciphered value;

receiving circuitry for receiving said enciphered value from said first location;

comparing instructions for comparing said expected enciphered value to said enciphered value; and

authentication generating instructions for generating a authentication signal in the event that said expected enciphered value matches said enciphered value.

42. The system of Claim 21, further comprising logic circuitry for XOR-ing said enciphered and processed communication signals with clear processed communication signals for preventing propagation of single bit errors that arise during enciphering from beyond the location at which they occur from said first signal processing circuit to said second signal processing circuit.

43. A communications controller circuit for privately communicating communication signals over a wireless communications network, comprising:

a signal processing circuit within said communications controller circuit for processing communications signals to form processed communication signals and further enciphering said processed communication signals; and

a transceiver circuit associated with said communications controller for transmitting said enciphered and processed communication signals from said communications controller circuit.

44. The controller circuit of Claim 43, wherein said signal processing circuit comprises a digital signal processing circuit.

45. The controller circuit of Claim 43, further comprising an enciphering algorithm embedded within said signal processing circuit for enciphering said processed communication signals.

46. The controller circuit of Claim 45, further comprising a deciphering algorithm within said signal processing circuit for deciphering processed communication signals received from a second communications controller circuit.

47. The controller circuit of Claim 45, wherein said signal processing circuit further comprises circuitry and instructions for embedding said enciphering algorithm in said signal processing circuit after manufacturing said communications controller circuit.

48. The controller circuit of Claim 43, wherein said signal processing circuit comprises circuitry and instructions for embedding an F enciphering algorithm in said signal processing circuit.

49. The controller circuit of Claim 43, wherein said signal processing circuit comprises circuitry and instructions for embedding a DES enciphering algorithm in said signal processing circuit.

50. The controller circuit of Claim 43, wherein said signal processing circuit comprises circuitry and instructions for embedding a BONUS enciphering algorithm in said signal processing circuit.

51. The controller circuit of Claim 43, wherein said signal processing circuit comprises circuitry and instructions for enciphering said processed communication signals in said signal processing circuit by programmably selecting an enciphering algorithm.

52. The controller circuit of Claim 41, wherein said signal processing circuit further comprises circuitry and instructions for programmably selecting the enciphering algorithm from among the group consisting essentially of an F enciphering algorithm a DES enciphering algorithm and a BONUS enciphering algorithm.

53. The controller circuit of Claim 48, further comprising a deciphering algorithm embedded within said second signal processing circuit for deciphering said processed communication signals.

54. The controller circuit of Claim 49, wherein said second communications controller circuit further comprises circuitry and instructions for embedding said deciphering algorithm within said second signal processing circuit after manufacturing said second communications controller circuit.

55. The controller circuit of Claim 50, wherein said deciphering algorithm comprises an F deciphering algorithm embedded within said second signal processing circuit for deciphering communications signals first enciphered using an F enciphering algorithm.

56. The controller circuit of Claim 51, wherein said deciphering algorithm comprises a DES deciphering algorithm embedded within said second signal processing circuit for deciphering communications signals first enciphered using a DES enciphering algorithm.

57. The controller circuit of Claim 51, wherein said deciphering algorithm comprises a BONUS deciphering algorithm embedded within said second signal processing circuit for deciphering communications signals first enciphered using a BONUS enciphering algorithm.

58. The controller circuit of Claim 43, further comprising circuitry and instructions within said signal processing circuit for authenticating communications between said location and said second location:

instructions within said communications controller circuit for generating a location identifier;

receiving circuitry associated with said communications controller for receiving a randomly generated number from said second location;

privacy instructions embedded within said signal processing circuit for employing a privacy function on said randomly generated number and said location identifier at said to generate an enciphered value; and

communications circuitry for directing said enciphered value to said second communications controller circuit.

59. The controller circuit of Claim 54, further comprising within said second communications controller circuit instructions for authenticating said generated authentication signals from said location said authenticating instructions, comprising:

identifier generating instructions for generating said location identifier;

random number generating instructions for randomly generating said randomly generated number;

privacy function instructions for transforming said randomly generated number and said location identifier into an expected enciphered value;

receiving circuitry for receiving said enciphered value from said location;

comparing instructions for comparing said expected enciphered value to said enciphered value; and

authentication generating instructions for generating an authentication signal in the event that said expected enciphered value matches said enciphered value.

60. The controller circuit of Claim 45, further comprising logic circuitry for XOR-ing said enciphered and processed communication signals with clear processed communication signals for preventing propagation of single bit errors beyond the location at which they occur as a consequence of the enciphering process from said signal processing circuit to said second signal processing circuit.